# 日　本　国　特　許　庁
## JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　５月　８日

出願番号
Application Number: 特願２００１－１３６８２７

出願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

USSN 09/940,594
MATTINGLY, STANGER, MALUR & BRUNDIDGE
(703) 684-1120
ASA-1029

２００１年　８月３１日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０７７４９０

【書類名】　特許願
【整理番号】　K01000831A
【あて先】　特許庁長官
【国際特許分類】　G06F 17/60
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
【氏名】　冨田　民則
【発明者】
【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共システム事業部内
【氏名】　宮崎　豊
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタル署名検証装置

【特許請求の範囲】

【請求項１】

少なくともその一部にデジタル署名が施された部分データを含むデジタル署名データを入力するデジタル署名検証装置において、

前記デジタル署名データを入力する手段と、

前記デジタル署名データに含まれる、前記部分データの範囲を識別する識別子に基づいて、前記部分データの範囲を検知する手段と、

検知された前記部分データの内容を表示する手段とを有することを特徴とするデジタル署名検証装置。

【請求項２】

請求項１に記載のデジタル署名検証装置において、

入力された前記デジタル署名データに施されたデジタル署名に関する情報を検出する手段を、さらに有し、

前記表示する手段は、検出された前記デジタル署名に関する情報を表示することを特徴とするデジタル署名検証装置。

【請求項３】

請求項２に記載のデジタル署名検証装置において、

前記デジタル署名に関する情報は、前記デジタル署名を施した主体に関する情報であることを特徴とするデジタル署名検証装置。

【請求項４】

請求項２または３のいずれかに記載のデジタル署名検証装置において、

前記表示する手段は、前記部分データの内容と前記デジタル署名に関する情報を関連付けて表示することを特徴とするデジタル署名検証装置。

【請求項５】

請求項４に記載のデジタル署名検証装置において、

前記表示する手段は、前記部分データの内容を示す情報を他の情報と区別して表示することを特徴とするデジタル署名検証装置。

【請求項６】

請求項１乃至５のいずれかに記載のデジタル署名検証装置において、

前記デジタル署名は、ＸＭＬにより記述され、

前記検知する手段は、所定のデータを指し示すものであって、ＸＭＬにより規定された前記識別子を検索し、検索された前記識別子に基づいて検知することを特徴とするデジタル署名検証装置。

【請求項７】

コンピュータに対して、

少なくともその一部にデジタル署名が施された部分データを含むデジタル署名データを入力する機能と、

前記デジタル署名データに含まれる、前記部分データの範囲を識別する識別子に基づいて、前記部分データの範囲を検知する機能と、

検知された前記部分データの内容を表示する機能を実行させるコンピュータプログラム。

【請求項８】

請求項７に記載のコンピュータプログラムにおいて、

入力された前記デジタル署名データに施されたデジタル署名に関する情報を検出する機能を、さらに前記コンピュータに実行させ、

前記表示する機能は、検出された前記デジタル署名に関する情報を表示することを特徴とするコンピュータプログラム。

【請求項９】

請求項８に記載のコンピュータプログラムにおいて、

前記デジタル署名に関する情報は、前記デジタル署名を施した主体に関する情報であることを特徴とするコンピュータプログラム。

【請求項１０】

請求項８または９のいずれかに記載のコンピュータプログラムにおいて、

前記表示する機能は、前記部分データの内容と前記デジタル署名に関する情報を関連付けて表示することを特徴とするデジタル署名検証装置。

【請求項１１】

請求項１０に記載のコンピュータプログラムにおいて、

前記表示する機能は、前記部分データの内容を示す情報を他の情報と区別して表示することを特徴とするコンピュータプログラム。

【請求項１２】

請求項７乃至１１のいずれかに記載のコンピュータプログラムにおいて、

前記デジタル署名は、ＸＭＬにより記述され、

前記検知する手段は、所定のデータを指し示すものであって、ＸＭＬにより規定された前記識別子を検索し、検索された前記識別子に基づいて検知することを特徴とするコンピュータプログラム。

【請求項１３】

電子データに対して、デジタル署名を施すデジタル署名データ作成装置において、

プログラムが格納された記憶装置と、

前記記憶装置と接続され、前記プログラムに従って、前記電子データに含まれる部分データに対しデジタル署名を施し、前記部分データを特定する識別子を生成し、前記デジタル署名が施された部分データおよび前記識別子を含むデジタル署名データを作成する処理装置を備えたことを特徴とするデジタル署名データ作成装置。

【請求項１４】

請求項１３に記載のデジタル署名データ作成装置において、

前記処理装置と接続され、ネットワークを介して情報処理装置と接続され、前記ネットワークを介して前記情報処理装置へ、作成された前記デジタル署名データを送信するネットワーク接続装置を、さらに備えたことを特徴とするデジタル署名データ作成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル署名を検証する技術に関する。より詳しくは、少なくともひとつのデジタル署名されたデータを表示することが可能な技術に関する。

【０００２】

【従来の技術】

官公庁や自治体、民間企業などの組織体の間で取り交わされる契約書などの書類に対して、紙によるやり取りに代えてコンピュータ等の情報処理装置を利用して作成した電子文書によるやり取りをすることが増えている。この電子文書のやり取りに当たり、本人性の保証や他者等による改ざんの防止のために電子的な署名（デジタル署名）が利用されつつある。デジタル署名自体の技術については、たとえば「ディジタル署名と暗号技術」１９９７年刊（ピアソン・エデュケーション）P90～95に記載されている。

【０００３】

また、デジタル署名されたデータに対してさらにデジタル署名を行う多重署名や、データの特定の部分にのみデジタル署名を行う部分署名の方式も種々提案されている。それらを活用して複数のデジタル署名が可能である。

【０００４】

デジタル署名されていることを表示する方法としては、たとえば「Ｗｅｂセキュリティ＆コマース」１９９８年刊（オライリー・ジャパン）P173～183に記述されているAuthenticode技術がある。本技術は、署名を検出すると証明書を表示する方式である。また、多重署名の状態を表示する技術としては、特開平2000-293102「デジタル多重署名装置および記憶媒体」で示される多重署名装置がある。

【０００５】

【発明が解決しようとする課題】

しかしながら、上述の公知例ではデジタル署名されていることを表示する際に、署名対象のデータに関する情報としてファイル名しか表示されないため。このために、署名対象のデータの内容をすぐに確認することが出来ないという問題がある。

【０００６】

また、近年注目されているＸＭＬ（eXtensible Markup Langage）文書には、ファイル中の一部分を署名対象として指定した部分署名が可能である。しかし、

ファイル全体に対するデジタル署名を想定とした上述の従来技術では、部分署名とその署名対象のデータの内容をすぐに確認することは困難であった。

【０００７】

本発明では、デジタル署名とその署名対象となるデータ（ファイル）の内容を、容易に確認することを目的とする。

【０００８】

【課題を解決するための手段】

上記の目的を達成するために本発明では、以下の構成をとる。

デジタル署名の対象となるデータと当該デジタル署名の対象となる範囲を示す情報を対応付けるものである。ここで、デジタル署名の対象となるデータは、所定の単位中の部分データであってもよい。所定の単位の１例としては１つのファイルがある。

【０００９】

本発明には、以下の構成も含まれる。

デジタル署名の対象となる範囲を示す情報として、デジタル署名対象データ識別子を、デジタル署名ファイルに添付することが含まれる。また、入力されるデジタル署名ファイルに添付されたデジタル書名対象データ識別子に基づいて、デジタル署名の対象となる範囲（部分データ）を検知する。デジタル署名の対象となる範囲の検知には、デジタル署名ファイルを解析し、どのようなデータが含まれるかを検知することが含まれる。

【００１０】

これらの処理の結果に基づいて、デジタル署名の対象となる範囲の内容とデジタル署名に関するデータを関連付けて表示することも、本発明に含まれる。デジタル署名に関するデータには、デジタル署名を行った装置もしくは利用者に関する情報が含まれる。また、関連付けた表示としては、同じディスプレイ上に表示することが含まれる。

【００１１】

【発明の実施の形態】

以下に、デジタル署名の表示を行う実施形態におけるデジタル署名表示装置に

ついて説明する。

図２は、本実施形態のデジタル署名表示装置の概略構成を示す図である。図２に示すように本実施形態のデジタル署名表示装置は、ＣＰＵ２０１とメモリ２０２と、磁気ディスク装置２０３と、入力装置２０４と、ディスプレイ装置２０５と、ネットワーク接続装置２０６とを有している。

【００１２】

ＣＰＵ２０１は、デジタル署名表示装置全体の動作、処理を制御するものである。メモリ２０２は、デジタル署名表示装置全体の動作を制御する際に、その為の各種処理プログラムやデータをロードする記憶装置である。

【００１３】

磁気ディスク装置２０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置２０４は、デジタル署名表示装置への操作指示等を入力する装置である。ディスプレイ装置２０５は、デジタル署名表示装置の動作状況や、デジタル署名状況を表示する装置である。ネットワーク接続装置２０６は、デジタル署名表示装置をネットワークに接続し、ネットワークに接続されたほかの装置とデータのやり取りを行う装置である。

【００１４】

また、デジタル署名表示装置は、デジタル署名解析処理部２１０とデジタル署名表示画面生成処理部２１１を有している。

【００１５】

デジタル署名解析処理部２１０は、入力装置２０４によって指定されたデジタル署名ファイルを入力し、デジタル署名の対象となるデータや、デジタル署名の有効性の検証、デジタル署名者等の情報を解析し、解析結果を出力する処理部である。

【００１６】

デジタル署名表示画面生成処理部２１１は、前記デジタル署名解析処理部２１０の出力した解析結果を入力し、デジタル署名表示画面を生成しディスプレイ装置２０５に表示する処理を行う処理部である。

【００１７】

デジタル署名表示装置をデジタル署名解析処理部２１０およびデジタル署名表示画面生成処理部２１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記憶媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。また、プログラムは、ネットワークを介して配信されてもよい。

【００１８】

デジタル署名は、たとえば標準化団体であるＷ３Ｃによって策定中の、ＸＭＬ－Ｓｉｇｎａｔｕｒｅという仕様を用いてもよい。図５に、ＸＭＬに準拠したデジタル署名ファイルの例ｄｓｉｇｎ．ｘｍｌを示す。本デジタル署名ファイルは、タグ<Signature>から</Signature>までの００１行目から０２３行目でデジタル署名情報を示す。００５行目のタグ<Reference>中で指定されている署名対象データ識別子５０１「ALL」は、署名対象データを識別する識別子である。前記識別子５０１「ALL」の示すデータは、本デジタル署名ファイル中の０２４行目のタグ<Object Id="ALL">から０４７行目の</Object>で囲まれる部分である。

【００１９】

図３は、本実施形態におけるデジタル署名表示装置のデジタル署名解析処理部２１０の処理手順を示すフローチャートである。図３に示すようにデジタル署名解析処理部２１０は、入力装置２０４から入力される、デジタル署名ファイル名を入力し、デジタル署名を解析する処理を行う。

【００２０】

以下、図５に示すデジタル署名ファイルｄｓｉｇｎ．ｘｍｌが指定された場合を例に処理を説明する。

ステップ３０１で前記指定された図５に示すデジタル署名ファイルｄｓｉｇｎ．ｘｍｌを、磁気ディスク装置２０３から読み込み、ファイルからデジタル署名を検索する。本実施形態では、タグ<Signature>と</Signature>で囲まれるデータを検索することでデジタル署名の存在を認識する。

【００２１】

ステップ３０２では、前記指定されたデジタル署名ファイル中にデジタル署名

が存在しないか、もしくは解析済みのデジタル署名しか存在しない場合は、処理を終了する。解析していないデジタル署名が検出されたら、ステップ３０３に進む。

【００２２】

ステップ３０３では、検出されたデジタル署名を解析し、デジタル署名対象データを検索する。図５のデジタル署名ファイルでは、００４行目の<Reference IDREF="ALL">タグに示されるデジタル署名対象データ識別子“ALL”が示すデータを検索する。検索の結果、デジタル署名ファイル中の０２３行目<Object ID="ALL">から０４７行目</Object>が署名対象データであると認識する。ここで、識別子は特定のデータを指し示すデータであり、識別子の示すデータが前記デジタル署名ファイルの外部であってもかまわない。その場合、デジタル署名対象データ識別子はたとえばＵＲＩ形式で表記する。

以降、デジタル署名対象データが含まれるファイルをデジタル署名データファイルと呼ぶ。

【００２３】

ステップ３０４では、デジタル署名の検証を行い、デジタル署名が正当なものであるかどうかを判定するとともに、署名作成者の情報を取得する。図５のデジタル署名ファイルｄｓｉｇｎ．ｘｍｌでは、０１６行目<X509Name></X509Name>タグによってはさまれる部分「CN=Tomita Taminori,O=Hitachi,C=JP」に署名作成者の情報が記述されている。

【００２４】

ステップ３０５では、ステップ３０３で確定した、前記デジタル署名対象データの領域と、デジタル署名対象データファイル名と、ステップ３０４で取得した署名作成者、署名検証結果をデジタル署名解析結果として出力する。

【００２５】

図６に、デジタル署名解析結果の例を示す。図６に示すように、デジタル署名ファイル名、署名作成者情報、デジタル署名対象データファイル名、署名対象データ識別子、署名検証結果から構成される。

【００２６】

デジタル署名解析結果出力後、再びステップ３０２に戻り、未解析のデジタル署名が存在する場合は、ステップ３０３からステップ３０５を繰り返す。デジタル署名ファイル中に存在するデジタル署名の解析を完了したら、処理を終了する。処理の終了は、対象となるデジタル署名全ての解析の完了を条件としてもよい。

【００２７】

デジタル署名解析処理部２１０の処理終了後、デジタル署名表示画面生成処理部２１１の処理が開始される。図４に示すようにデジタル署名表示画面生成処理部２１1は、前記デジタル署名解析処理部２１０が出力した、デジタル署名解析結果を入力し、デジタル署名対象を表示する画面を生成する処理を行う。

【００２８】

ステップ４０１では、前記デジタル署名解析処理部の出力した、前記デジタル署名解析結果を入力する。

【００２９】

ステップ４０２では、前記デジタル署名解析結果に未表示のデジタル署名解析結果が存在しない場合は、処理を終了する。表示していないデジタル署名が存在する場合は、ステップ４０３に進む。

【００３０】

ステップ４０３では、前記未表示のデジタル署名解析結果に示される、デジタル署名対象データファイルを表示する。既に前記デジタル署名対象データファイルが表示されている場合は、本処理は省略する。図６の例におけるデジタル署名対象データファイルｄｓｉｇｎ．ｘｍｌの表示例を、図７に示す。

【００３１】

ステップ４０４では、ステップ４０３で表示されたデジタル署名対象データファイルのうち、デジタル署名対象データの領域を示す枠を生成する。図６の例における表示例を、図８に示す。図中１０１はデジタル署名対象データの領域を示す枠である。

【００３２】

ステップ４０５では、ステップ４０４で表示された、前記デジタル署名対象デ

ータの領域を示す枠が示すデジタル署名の署名解析結果を表示する。図６の例における表示例を図１に示す。図中１０１はデジタル署名対象データの領域を示す枠、１０２は前記枠１０１が示すデジタル署名の解析結果の表示である。

【００３３】

署名解析結果の表示方法は、図１に示したように文字列で表示する以外にも、色や、記号で表示してもよい。

また、たとえば前記表示枠１０１の色によって、署名検証結果を表現することにしても良い。

【００３４】

ステップ４０５終了後、再びステップ４０２に戻り、未表示のデジタル署名解析結果が存在する場合は、ステップ４０３からステップ４０５を繰り返す。デジタル署名解析結果の画面生成を完了したら、処理を終了する。処理の終了は、全てのデジタル署名解析結果の画面生成を完了したことを条件としてもよい。

【００３５】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名者の情報と、その署名対象のデータの内容を一つの画面上に表示するためどのような内容が、何者によってデジタル署名されているのかを多くの操作なしに確認することができる。

【００３６】

なお、本実施形態ではデジタル署名解析処理部２１０と、デジタル署名表示画面生成処理部２１１が、同一の装置で実現されているが、それぞれ別の装置で実現されてもかまわない。

【００３７】

図９は、ＸＭＬによって記述された第二のデジタル署名ファイルｄｓｉｇｎ２．ｘｍｌの例である。

【００３８】

第二のデジタル署名ファイルはタグ<Signature>から</Signature>までの００２行目から０２３行目までの第一のデジタル署名９０１と、０２４行目から０４５行目までの第二のデジタル署名９０３を含む。

【００３９】

図９中タグ署名対象データ識別子９０２は、第一のデジタル署名９０１の署名対象データを識別する識別子である。識別子９０２は、タグ<Reference>中で指定されている。識別子９０２の示すデータは、図５のファイルｄｓｉｇｎ．ｘｍｌ中の０２５行目のタグ<Object Id="auther">から０３３行目の</Object>で囲まれる部分である。なお、識別子９０２は、具体的な例としては、" http://home/dsign.html#author "がある。

【００４０】

同様に、図９の署名対象識別子９０４は、第二のデジタル署名９０３の署名対象データを識別する識別子である。署名対象識別子９０４の示すデータは、図５のファイルｄｓｉｇｎ．ｘｍｌ中の０３４行目のタグ<Object Id="title">から０４５行目の</Object>で囲まれる部分である。なお、署名対象識別子９０４は、具体的な例としては、"http://home/dsign.html#title"がある。

【００４１】

このような第二のデジタル署名ファイルを、前記デジタル署名解析処理部２１０で処理した結果を図１０に示す。

【００４２】

図１０は、第二のデジタル署名ファイルのデジタル署名解析結果である。図中１００１は第一のデジタル署名９０１のデジタル署名解析結果、図中１００２は第二のデジタル署名９０３のデジタル署名解析結果である。

【００４３】

次に、図１０に示すデジタル署名解析結果を、前記デジタル署名表示画面生成処理部２１１で処理し、デジタル署名表示画面を生成する。

【００４４】

図１１に、第二のデジタル署名ファイルの表示画面例を示す。表示枠１１０１は第一のデジタル署名９０１の署名対象範囲、署名情報１１０２は第一のデジタル署名９０１の署名解析結果に関する情報である。同様に表示枠１１０３は第二のデジタル署名９０３の署名対象範囲、署名情報１１０４は第二のデジタル署名９０３の署名解析結果に関する情報である。

【００４５】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名対象のデータがファイルの一部であっても、デジタル署名対象ファイルの内容と、デジタル署名対象の領域と、デジタル署名者の情報を一つの画面上に表示するためどのような内容が、何者によってデジタル署名されているのかを多くの操作なしに確認することができる。また一つの署名対象ファイルに対して複数の署名者が署名をした場合でも同様に多くの操作なしに確認することができる。

【００４６】

図１２は、ＸＭＬによって記述された第三のデジタル署名ファイルｄｓｉｇｎ３．ｘｍｌの例である。

【００４７】

第三のデジタル署名ファイルは００２行目から０１８行目までの第一のデジタル署名１２０１と、０２０行目から０３６行目までの第二のデジタル署名１２０３を含む。

【００４８】

前記第一のデジタル署名１２０１の署名対象データは０１９行目から０４９行目の識別子「ALL」で示される領域１２０２で、同様に前記第二のデジタル署名１２０３の証明対象データは０３７行目から０４８行目の識別子「title」で示される領域１２０４である。

【００４９】

この第三のデジタル署名ファイルを、前記デジタル署名解析処理部２１０で処理した結果を図１３に示す。

【００５０】

図１３は、第三のデジタル署名ファイルのデジタル署名解析結果である。図中１３０１は前記第一のデジタル署名１２０１のデジタル署名解析結果、図中１３０２は前記第二のデジタル署名１２０３のデジタル署名解析結果である。

【００５１】

次に、図１３に示すデジタル署名解析結果を、デジタル署名表示画面生成処理部２１１で処理し、デジタル署名表示画面を生成する。

【００５２】

図１４に、第三のデジタル署名ファイルの表示画面例を示す。表示枠１４０１は第一のデジタル署名１２０１の署名対象範囲、署名情報１４０２は第一のデジタル署名１２０１の署名解析結果に関する情報である。同様に表示枠１４０３は第二のデジタル署名１２０３の署名対象範囲、署名情報１４０４は第二のデジタル署名１２０３の署名解析結果に関する情報である。

【００５３】

表示枠１４０１と、１４０３の包含関係から、第一のデジタル署名１２０１は識別子「title」で示される領域と、第二のデジタル署名１２０３を含めたデータに対する署名であることが容易に確認することができる。

【００５４】

以上説明したように、本実施形態のデジタル署名表示装置によれば、デジタル署名対象のデータが複数のデジタル署名により多重署名されてあっても、デジタル署名対象の領域の包含関係によって、どのような内容が、何者によってデジタル署名されているのかを容易に確認することができる。

【００５５】

なお、本発明による署名対象データの領域の表示方法は、上述した実施形態に限定されるものではない。たとえば、実施形態にあった枠線の代わりに、画面背景の表示色を変えて表示してもよい。

【００５６】

また、本発明による署名情報の表示内容は、上述した実施形態に限定されるものではない。たとえば、実施形態の署名者情報および署名検証結果を表示してもよい。また、署名検証結果を表示してもよい。署名検証結果については、これを単独で表示してもよい。

【００５７】

また、本発明によるデジタル署名方式は、上述した実施形態に限定されるものではない。すくなくとも署名対象データと署名者の情報を特定する情報を有するすべてのデジタル署名方式に適用可能である。

【００５８】

すなわち、本発明は、デジタル署名を表現する手段において、デジタル署名されたデータを含むファイルの内容と、デジタル署名対象の領域と、署名情報を同一画面に表示する、という要旨を逸脱しない範囲で実施することができる。

【００５９】

また、本実施形態によれば、デジタル署名対象のデータを含むファイルの内容を表示し、その表示画面にデジタル署名対象の領域と、デジタル署名情報を二次元的に重ねて表示するので、部分署名、多重署名等の多様なデジタル署名の関係を、多くの操作なしに確認することが可能である。

【００６０】

【発明の効果】

本発明によれば、デジタル署名の対象となっているデータの内容を容易に把握することが可能になる。

【図面の簡単な説明】

【図１】本発明の実施形態のデジタル署名表示装置でデジタル署名データｄｓｉｇｎ．ｘｍｌを表示した図である。

【図２】本発明の実施形態のデジタル署名表示装置の概略構成を示す図である。

【図３】本発明の実施形態のデジタル署名解析処理部２１０の処理手順を示すフローチャートである。

【図４】本発明の実施形態のデジタル署名表示画面生成処理部２１１の処理手順を示すフローチャートである。

【図５】デジタル署名データｄｓｉｇｎ．ｘｍｌを示す図である。

【図６】デジタル署名データｄｓｉｇｎ．ｘｍｌをデジタル署名解析処理部２１０で処理した結果得られた、デジタル署名情報の例を示す図である。

【図７】デジタル署名データｄｓｉｇｎ．ｘｍｌの表示例を示す図である。

【図８】デジタル署名データｄｓｉｇｎ．ｘｍｌの表示例に、識別子ＡＬＬで示されるデータを示す枠を表示した図である。

【図９】デジタル署名データｄｓｉｇｎ２．ｘｍｌを示す図である。

【図１０】デジタル署名データｄｓｉｇｎ２．ｘｍｌをデジタル署名解析処理部２１０で処理した結果得られた、デジタル署名情報の例を示す図である。

【図１１】本発明の実施形態のデジタル署名表示装置でデジタル署名データｄｓｉｇｎ２．ｘｍｌを表示した図である。

【図１２】デジタル署名データｄｓｉｇｎ３．ｘｍｌを示す図である。

【図１３】デジタル署名データｄｓｉｇｎ３．ｘｍｌをデジタル署名解析処理部２１０で処理した結果得られた、デジタル署名情報の例を示す図である。

【図１４】本発明の実施形態のデジタル署名表示装置でデジタル署名データｄｓｉｇｎ３．ｘｍｌを表示した図である。

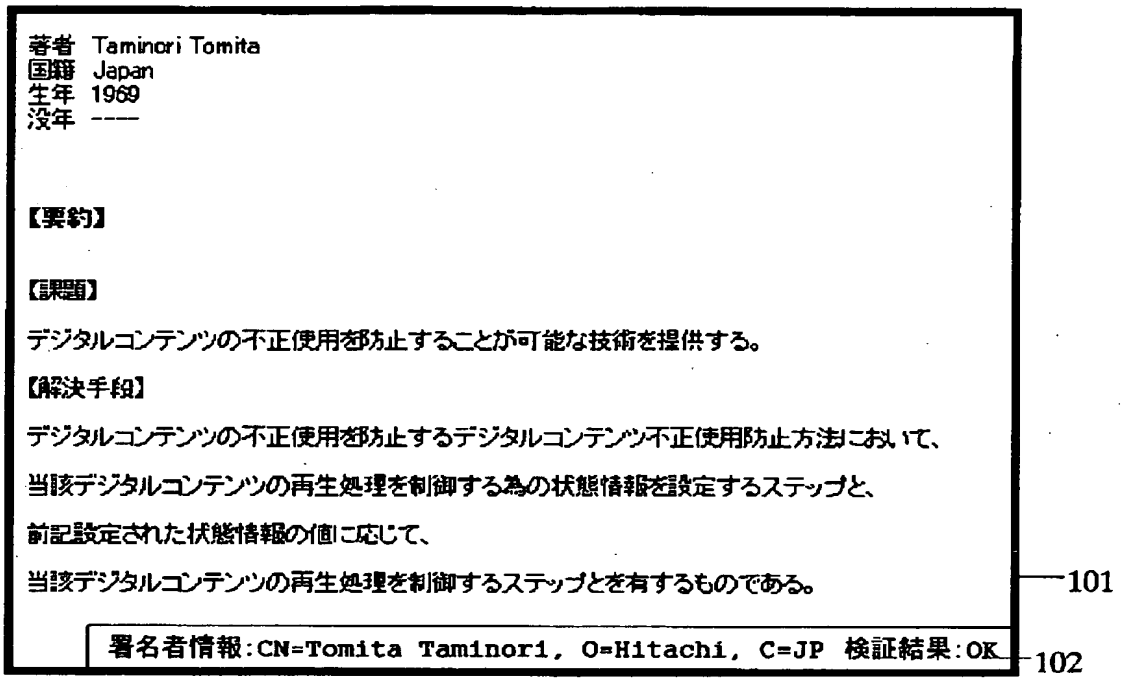
【符号の説明】

１０１…デジタル署名対象データの領域を示す枠、１０２…デジタル署名データｄｓｉｇｎ．ｘｍｌにおける署名解析結果に関する情報の表示、２１０…デジタル署名解析処理部、２１１…デジタル署名表示画面生成処理部、１１０１…デジタル署名データｄｓｉｇｎ２．ｘｍｌにおける第一のデジタル署名対象データの領域を示す枠、１１０２…デジタル署名データｄｓｉｇｎ２．ｘｍｌにおける第一の署名解析結果に関する情報の表示、１１０３…デジタル署名データｄｓｉｇｎ２．ｘｍｌにおける第二のデジタル署名対象データの領域を示す枠、１１０４…デジタル署名データｄｓｉｇｎ２．ｘｍｌにおける第二の署名解析結果に関する情報の表示、１４０１…デジタル署名データｄｓｉｇｎ３．ｘｍｌにおける第一のデジタル署名対象データの領域を示す枠、１４０２…デジタル署名データｄｓｉｇｎ３．ｘｍｌにおける第一の署名解析結果に関する情報の表示、１４０３…デジタル署名データｄｓｉｇｎ３．ｘｍｌにおける第二のデジタル署名対象データの領域を示す枠、１４０４…デジタル署名データｄｓｉｇｎ３．ｘｍｌにおける第二の署名解析結果に関する情報の表示

【書類名】　図面

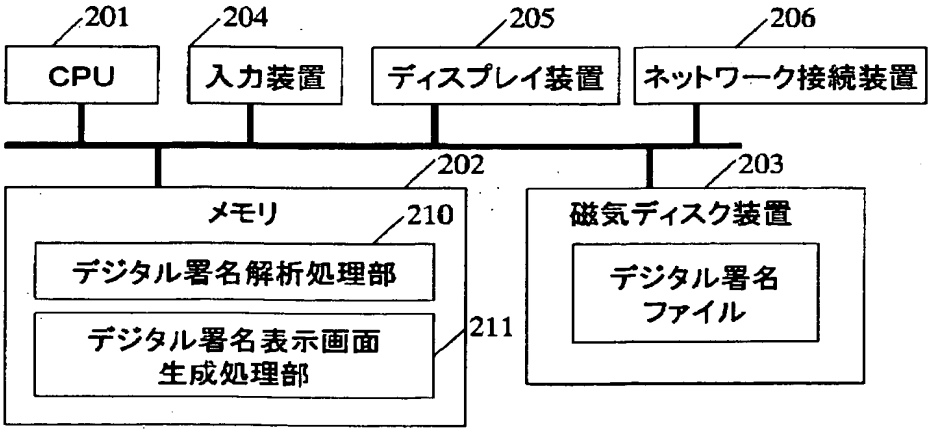
【図１】

図１



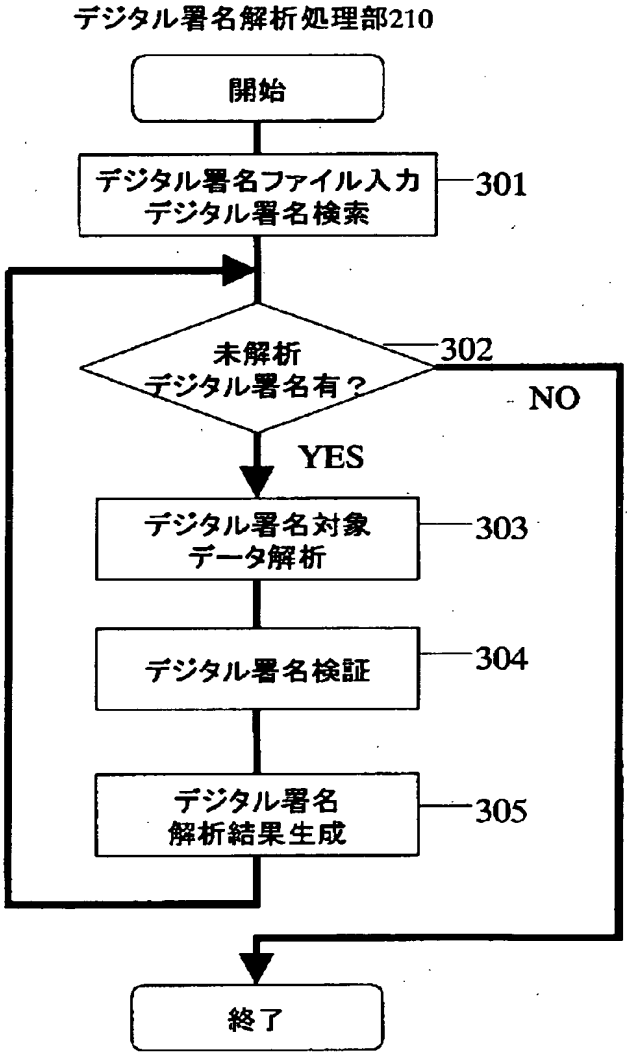

【図２】

図２



【図３】

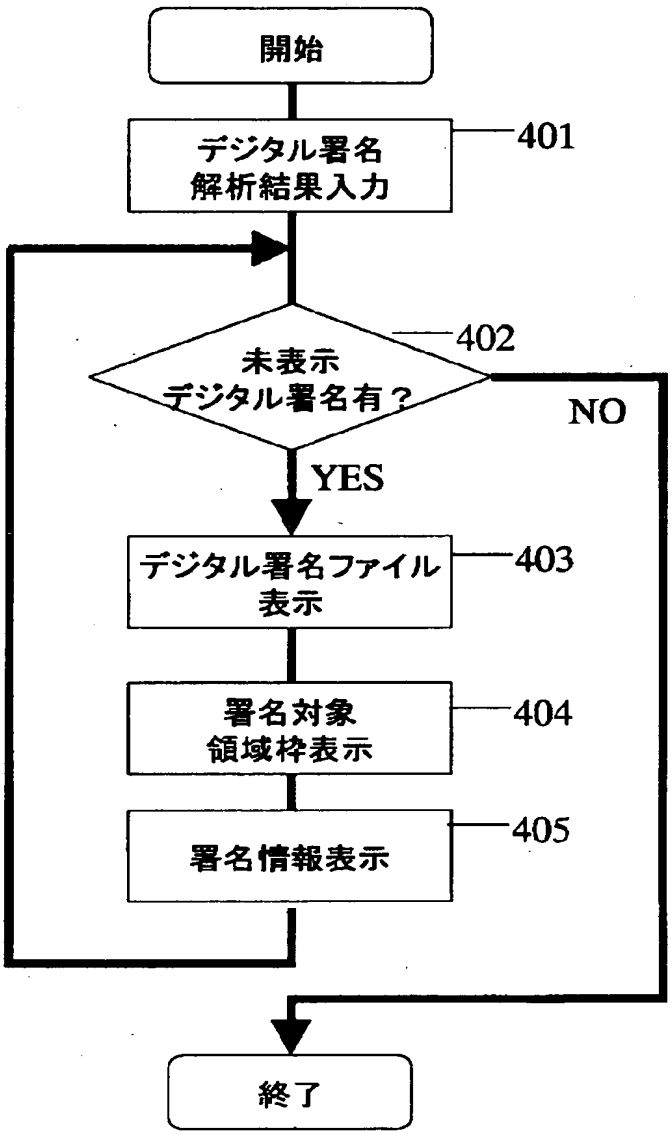
図3


デジタル署名解析処理部210
開始
デジタル署名ファイル入力
デジタル署名検索
301
未解析
デジタル署名有？
302
NO
YES
デジタル署名対象
データ解析
303
デジタル署名検証
304
デジタル署名
解析結果生成
305
終了

【図４】

図4

画面生成処理部211



【図５】

図5

dsign.xml

```
001 <document>
002  <Signature>                                    501
003   <SignedInfo>                                 /
004     <SignatureMethod Algorithm="http://. . ."/>
005     <Reference IDREF="ALL">
006       <DigestMethod Algorithm="http://. . ."/>
007       <DigestValue Encoding=". . .">
008         WfKRfGWiAni9bY9k/sXgBFt4ge4=
009       </DigestValue>
010     </Reference>
011   </SignedInfo>
012   <SignatureValue>
013     MCwCFB0M62GxrrxMGm7qfBt8R+Zv4YuIAhRvQH1DkgAdtnDQIOYOg07srWha1A==
014   </SignatureValue>
015   <KeyInfo>
016     <X509Data>
017       <X509Name>CN=Tomita Taminori, O=Hitachi, C=JP</X509Name>
018       <X509Certificate>
019 tLKJqNhJznnUvkqZQ2ce+6slau1J8cw7yALDZJhzfFlhHzALBgcqhkjOOAQDBQADLwAwLAIUZUJD
020       </X509Certificate>
021     </X509Data>
022   </KeyInfo>
023  </Signature>
024  <Object ID="ALL">
025   <Object Id="author">
026     <author>
027       <last-name>Tomita</last-name>
028       <first-name>Taminori</first-name>
029       <nationality>Japan</nationality>
030       <year-of-birth>1969</year-of-birth>
031       <year-of-death>----</year-of-death>
032     </author>
033   </Object>
034   <Object Id="tilte">
035    <title>【要約】</title>
036    <lines>
037      <line>【課題】
038      <line>デジタルコンテンツの不正使用を防止することが可能な技術を提供する。</line>
039      <line>【解決手段】</line>
040      <line>デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、</line>
041      <line>当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、</line>
042      <line>前記設定された状態情報の値に応じて、</line>
043      <line>当該デジタルコンテンツの再生処理を制御するステップとを有するものである。</line>
044    </lines>
045   </Object>
046  </Object>
047 </document>
```

【図６】

図6

| # | デジタル署名ファイル名 | 署名者作成者情報 | デジタル署名対象データファイル名 | 署名対象データ識別子 | 署名検証結果 |
|---|---|---|---|---|---|
| 1 | dsign.xml | CN=Tomita Taminori, O=Hitachi, C=JP | dsign.xml | ALL | OK |

【図７】

図7

著者 Taminori Tomita
国籍 Japan
生年 1969
没年 ----

【要約】

【課題】

デジタルコンテンツの不正使用を防止することが可能な技術を提供する。

【解決手段】

デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、

当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、

前記設定された状態情報の値に応じて、

当該デジタルコンテンツの再生処理を制御するステップとを有するものである。

【図８】

図8

著者 Taminori Tomita
国籍 Japan
生年 1969
没年 ——

【要約】

【課題】

デジタルコンテンツの不正使用を防止することが可能な技術を提供する。

【解決手段】

デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、

当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、

前記設定された状態情報の値に応じて、

当該デジタルコンテンツの再生処理を制御するステップとを有するものである。

101

【図９】

図9

dsign2.xml

```
001 <document>
002   <Signature>
003    <SignedInfo>
004      <SignatureMethod Algorithm="http://. . ."/>
005      <Reference IDREF="http://home/dsign.html#author">
006        <DigestMethod Algorithm="http://. . ."/>
007        <DigestValue Encoding=". . .">
008          bY3JsOGI6Nd6ddsafT9FAn++2uK9gBFt4ge4=
009        </DigestValue>
010      </Reference>
011    </SignedInfo>
012    <SignatureValue>
013      4eX1QCDRKrxFr/bY3JsOGI6Nd6afT9FAn++2uK9yWegTSmM6aiAqmb0Eiybf50q7d
014    </SignatureValue>
015    <KeyInfo>
016      <X509Data>
017        <X509Name>CN=Taminori Tomita, C=JP</X509Name>
018        <X509Certificate>
019 tLKvkqZQ2ce+6slau1J6slau1J8cw7yALDZJhzfFlhHzALBgcqhkjwLAIUZUJD
020        </X509Certificate>
021      </X509Data>
022    </KeyInfo>
023  </Signature>
024   <Signature>
025    <SignedInfo>
026      <SignatureMethod Algorithm="http://. . ."/>
027      <Reference IDREF="http://home/dsign.html#title">
028        <DigestMethod Algorithm="http://. . ."/>
029        <DigestValue Encoding=". . .">
030          hkjOOAQDBQADLwAwLAIUZUJD++2uK9gBFt4ge4=
031        </DigestValue>
032      </Reference>
033    </SignedInfo>
034    <SignatureValue>
035      6slau1J8cw7yALDZJhzfFlhHzALBgcqhkjOOAQDBQADLwAwLAIUZUJDAqmb0Eiybf50q7d
036    </SignatureValue>
037    <KeyInfo>
038      <X509Data>
039        <X509Name>CN=Taro Yamada, O=Hitachi syuppann, C=JP</X509Name>
040        <X509Certificate>
041 Ydoysr2us1eZ9p6xRwEZYnoCFC97/v+w6FIyM+KgDDAgK9LYxN/n
042        </X509Certificate>
043      </X509Data>
044    </KeyInfo>
045  </Signature>
048 </document>
```

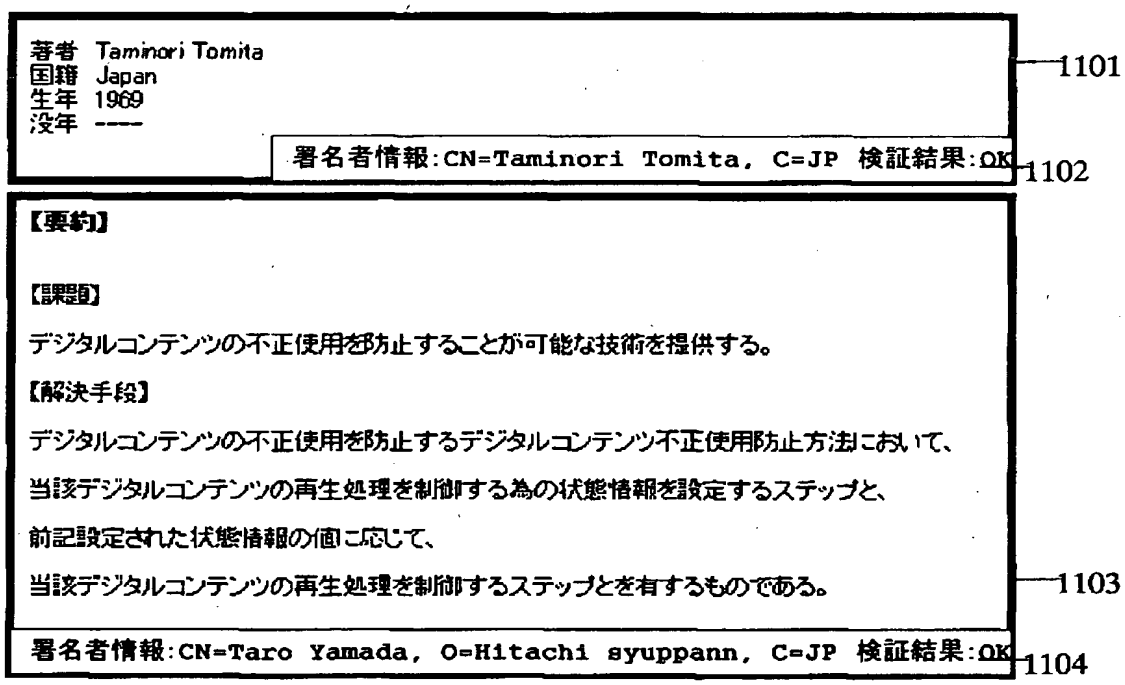
【図１０】

図10

| # | デジタル署名ファイル名 | 署名者作成者情報 | デジタル署名対象データファイル名 | 署名対象データ識別子 | 署名検証結果 |
|---|---|---|---|---|---|
| 1001 1 | dsign2.xml | CN=Taminori Tomita, C=JP | dsign.html | http://home/dsign.html#auther | OK |
| 1002 2 | dsign2.xml | CN=Taro Yamada, O=Hitachi syuppann, C=JP | dsign.html | http://home/dsign.html#title | OK |

【図１１】

図11



【図１２】

図12

dsign3.xml

```
001 <document>
002   <Signature>                                                    1201
003    <SignedInfo>
004      <SignatureMethod Algorithm="http://. . ."/>
005      <Reference IDREF="ALL">
006        . . .
007      </Reference>
008    </SignedInfo>
009    <SignatureValue>
010      MCwCFB0M62GxrrxMGm7qfBt8R+6slaulJ8cw7yALDZJhzfFlOg07srWha1A==
011    </SignatureValue>
012    <KeyInfo>
013      <X509Data>
014        <X509Name>CN=Taro Yamada, O=Hitachi syuppann, C=JP</X509Name>
015       . . .
016      </X509Data>
017    </KeyInfo>
018  </Signature>                                                     1202
019  <Object ID="ALL">
020    <Signature>                                                    1203
021     <SignedInfo>
022       <SignatureMethod Algorithm="http://. . ."/>
023       <Reference IDREF="tilte">
024         . . .
025       </Reference>
026     </SignedInfo>
027     <SignatureValue>
028       MCwCFB0M62GxrrxMGm7qfBt8R+Zv4YuIAhRvQHQIOYOg0
029     </SignatureValue>
030     <KeyInfo>
031       <X509Data>
032         <X509Name>CN=Taminori Tomita, C=JP</X509Name>
033       . . .
034       </X509Data>
035     </KeyInfo>
036   </Signature>                                                   1204
037   <Object Id="tilte">
038     <title>【要約】</title>
039     <lines>
040       <line>【課題】
041       <line>デジタルコンテンツの不正使用を防止することが可能な技術を提供する。</line>
042       <line>【解決手段】</line>
043       <line>デジタルコンテンツの不正使用を防止するデジタルコンテンツ不正使用防止方法において、</line>
044       <line>当該デジタルコンテンツの再生処理を制御する為の状態情報を設定するステップと、</line>
045       <line>前記設定された状態情報の値に応じて、</line>
046       <line>当該デジタルコンテンツの再生処理を制御するステップとを有するものである。</line>
047     </lines>
048   </Object>
049  </Object>
050 </document>
```

【図１３】

図13

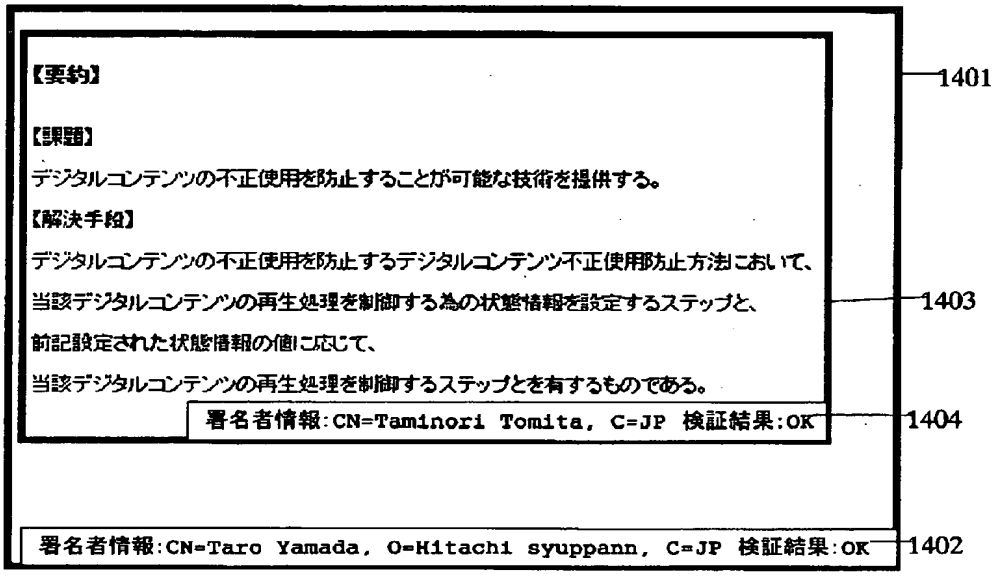
| # | デジタル署名ファイル名 | 署名者作成者情報 | デジタル署名対象データファイル名 | 署名対象データ識別子 | 署名検証結果 |
|---|---|---|---|---|---|
| 1 | dsign3.xml | CN=Taro Yamada, O=Hitachi syuppann, C=JP | dsign3.html | ALL | OK |
| 2 | dsign3.xml | CN=Taminori Tomita, C=JP | dsign3.html | title | OK |

1301

1302

【図１４】

図14



【書類名】　要約書

【要約】

【課題】

デジタル署名と署名対象データの内容の関係を容易に確認することが可能な装置を提供する。

【解決手段】

本発明のデジタル署名装置は、少なくとも署名対象のデータを識別する情報と、署名者を識別する情報が含まれるデジタル署名を含むファイルを入力し、前記デジタル署名と、前記デジタル署名の署名対象データの関係を解析し、署名の検証を行い、それらの署名解析結果を出力するデジタル署名解析手段と、前記署名対象データの内容と、前記署名解析結果を合わせて表示するデジタル署名表示画面を生成するデジタル署名表示画面生成手段とを備えるものであり、前記デジタル署名表示画面は署名対象データの内容とデジタル署名の情報を同一画面上に表示する。

【選択図】　図２



出証特２００１－３０７７４９０

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００１－１３６８２７ |
| 受付番号 | ５０１００６５７１８９ |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席　　００９６ |
| 作成日 | 平成１３年　５月　９日 |

＜認定情報・付加情報＞

【提出日】　平成13年 5月 8日

次頁無



出証特２００１－３０７７４９０

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所